AEAIM-C-P   14 May 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Accrediting Systems for Processing Focal Point Information

This memorandum expires in 1 year.

1. References:

    a. DOD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

    b. Chairman, Joint Chief of Staff, Manual 3213.02A, (C) Joint Staff Focal Point Communications System Procedures Manual (U), 31 January 1997, and change 1, 8 August 2003.

    c. Memorandum, Joint Staff, 8 August 2003, subject: Dissemination and Processing of Focal Point Information.

    d. DISA DMS Field Engineer Notice (FEN), 15 August 2003, DMS Configuration and Usage Guide for SPECAT and Other Special Handling Messages, 3.0.2-SPECAT-D01.

2. Commands, agencies, and organizations that use Focal Point systems have been directed by the Joint Staff to provide for local implementation and configuration of the Defense Message System (DMS) so that the DMS can be accredited for transmitting special category (SPECAT) messages (ref 1c).

3. Designated approving authorities (DAAs) will reaccredit DMS enclaves for processing Focal Point information according to reference 1c. DAAs and Focal Point officers will implement procedures to ensure appropriate protective measures are in place for distributing and processing information.

4. The USAREUR Information Assurance Program Manager (IAPM) will conduct certification testing and provide DAA certification statements to DMS service centers. Personnel appointed as information management officers will configure and maintain DMS client workstations. Focal Point officers and their designated trusted agents will administer local systems for processing, storing, and transmitting Focal Point information (refs 1a and d).

5. This policy will be implemented immediately according to the enclosure. References 1b and d provide implementation procedures for DAAs.

6. Requests for exception to this policy must be sent through the USAREUR G2 (AEAGB-SAD-SB) to the Joint Staff, J3/JOD, Room 2B885, The Pentagon, Washington, DC 20318-3000.

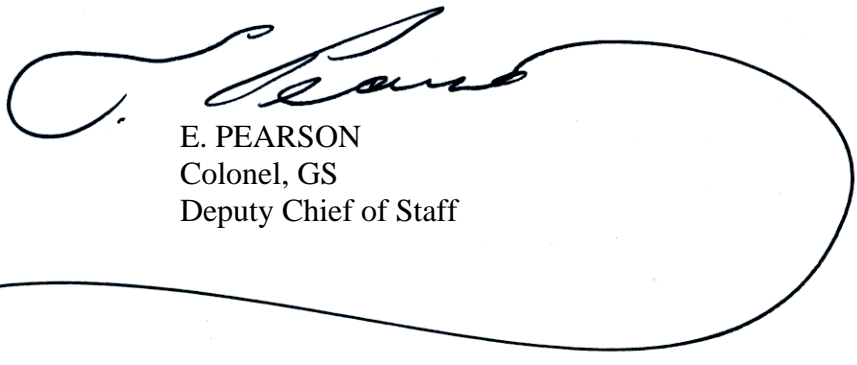*This memorandum is available at https://www.aeaim.hqusareur.army.mil/library/.*

AEAIM-C-P
SUBJECT: Accrediting Systems for Processing Focal Point Information

7. POCs for this policy are as follows:

    a. USAREUR G2, DSN 370-7574 or e-mail: usareurg2uc@dms.heidelberg.army.mil.

    b. USAREUR G3, DSN 370-6329 or e-mail: usareurg3uc@dms.heidelberg.army.mil.

    c. USAREUR IAPM, DSN 380-5813 or e-mail: iapm@hq.5sigcmd.army.mil.

FOR THE COMMANDER:

Encl   E. PEARSON
                           Colonel, GS
                           Deputy Chief of Staff

DISTRIBUTION:
C (AEPUBS)

FOCAL POINT INFORMATION POLICY AND PROCEDURES

1. PURPOSE
This enclosure provides policy on—

a. Storing, processing, and transmitting Focal Point information in the European theater.

b. Accrediting systems that store, process, or transmit Focal Point information on the LandWarNet (Class).

2. APPLICABILITY
This policy applies to USAREUR major subordinate and tenant commands (AE Reg 10-5, app A) and the United States Army Installation Management Agency, Europe Region Office.

3. REFERENCES

a. Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems, 5 June 1999.

b. Chairman, Joint Chief of Staff, Manual 3213.02A, (C) Joint Staff Focal Point Communications System Procedures Manual (U), 31 January 1997, and change 1, 8 August 2003.

c. Memorandum, Joint Staff, 8 August 2003, subject: Dissemination and Processing of Focal Point Information.

d. DISA DMS Field Engineer Notice (FEN), 15 August 2003, DMS Configuration and Usage Guide for SPECAT and Other Special Handling Messages, 3.0.2-SPECAT-D01.

4. POLICY
Focal Point messages will be distributed and processed using the Defense Message System (DMS). The following requirements must be met for DMS enclaves and end-users to be authorized to process Focal Point information:

a. Computer systems used to store, process, or transmit Focal Point information must have strong user-authentication capabilities, file-level permission controls, and other capabilities to password-protect files and e-mail messages.

(1) The minimum classification level for systems that process Focal Point information is Confidential.

(2) System users will have a security clearance that is at least equal to the classification of the system. Access to data entered into the system must be limited to personnel who have a "need to know."

Encl

(3) Unauthorized individuals who have physical access to the system must be under continuous supervision by authorized personnel.

(4) A backup system must be established for every system that processes Focal Point information. The backup system must have enough storage space and must allow for effective system restoration.

b. Organizational mailboxes designated for receiving only Focal Point messages must be created on the DMS server. Mailboxes must be configured according to reference 3d, section 5.1.2.2.1, *Setting Mailbox Permissions (Server)*. Access to mailboxes will be restricted to Focal Point officers and their designated trusted agents.

c. Local DMS service centers must create DMS directory entries identifying organizational Focal Point addresses and legacy Plain Language addresses for organization Focal Point accounts.

d. Mailbox and inbox permissions on local workstations must be set according to reference 3d, section 5.1.2.2.2, *Setting Mailbox Permissions (Client)*; and section 5.1.2.2.2.2, *Setting Inbox Permissions*.

e. Messages must be signed and encrypted before being sent.

f. Focal Point information stored on external media or printed must be marked and labeled according to reference 3a, paragraph 8.B.2.a.

5. AUTHORIZATION
Focal Point officers and designated trusted agents who meet the requirements in paragraph 4 of this enclosure will be authorized to process Focal Point information on the LandWarNet (Class).

6. EXCEPTIONS
Requests for exception to this policy must be sent through the USAREUR G2 (AEAGB-SAD-SB) to the Joint Staff (J3/JOD), Room 2B885, The Pentagon, Washington, DC 20318-3000.